UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/533,583	05/03/2005	Akiyoshi Okamoto	050252	4118

23850 7590 11/10/2009

KRATZ, QUINTOS & HANSON, LLP
1420 K Street, N.W.
Suite 400
WASHINGTON, DC 20005

EXAMINER	
AVERY, JEREMIAH L	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
11/10/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/533,583	OKAMOTO ET AL.	
	Examiner	Art Unit	
	JEREMIAH AVERY	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 July 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 May 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

I. Claim 20 has been added.

II. Claims 1-20 have been examined.

III. Responses to Applicant's remarks have been given.

Response to Arguments

1. The Applicant's amendments to the Abstract give cause for the objection to the Specification to be hereby withdrawn.

2. In response to Applicant's argument that the references fail to show certain features of Applicant's invention, it is noted that the features upon which Applicant relies (i.e., "The system of preventing unauthorized use recited in claim 1 allows 'easy distribution of the digital content,' e.g. of the claimed distributing recording medium by easy duplication of the digital content, while still providing a mechanism for reliable collection of charges associated with the secondary use of the digital content (Specification, paragraph 17)") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

3. With regards to the Applicant's arguments that "Ansell fails to disclose the recited digital content playing device", the Examiner respectfully disagrees and maintains the cited sections below. Further, Ansell discloses the necessary authentication means in order to properly utilize the "playing device" via the unique identifiers of the player as well as authenticating the "initiator" requesting the playback. When the authentication

process(es) produces a positive result, the device and requested data become readily available and usable. The data within Ansell (e.g. "a secure portable track (SPT)") has the necessary protections (e.g. cryptographic and tamper-resistant functions) to prevent unauthorized transferring or utilization of itself; which coincides with the Applicant's claim language of "a system for preventing unauthorized play of digital content". With the necessary protection means in place, the content can only be successfully accessed upon the completion of an authentication process and the subsequent authorization. Thus, Ansell's disclosure substantially discloses the prevention and protection means within the Applicant's claimed invention.

4. In response to the Applicant's argument that "Ansell also fails to disclose the invention recited in claims 2-9, 13-15 and 19", the Examiner maintains the cited grounds of rejection. Further, the Applicant's arguments regarding claims 10-12 and 16-18, the Examiner upholds that Ansell does disclose the "digital content playing device" as stated above. Also, the Applicant does not address how "Merkle does not cure the deficiencies of Ansell", thus the Examiner maintains that Merkle discloses the claim limitations, as cited below.

Claim Objections

5. Claims 1-12, 14 and 16-19 objected to because of the following informalities: grammatical error. These claims have the language "piece data". The Examiner recommends amending the language to be "piece of data". Appropriate correction is required.

Claim Rejections - 35 USC § 102

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-9, 13-15, 19 and 20 are rejected under 35 U.S.C. 102(b) as being anticipated by United States Patent No. 6,367,019 to Ansell et al., hereinafter Ansell.

6. Regarding claim 1, Ansell discloses a system for preventing unauthorized play of digital content comprising:

a distributing recording medium on which a content file having header information and a data body is recorded and lacks a part of the header information (column 5, lines 40-46, column 7, lines 65-67, column 8, lines 1-17, "parses header 302 therefrom and parses bindings 400 from header 302", column 11, lines 11-45, "specifying a type of restriction on playback of SPT 116", column 12, lines 56-67, "SPT 116 cannot be played back from any other storage medium unless cryptographic logic 1104 is accurately replicated" and column 13, lines 6-15);

a management unit for managing use of the content file on the distributing recording medium and capable of transferring the prepared part of the header information as a piece data via a communication line (column 2, lines 6-13, 28-34 and 52-67, column 3, lines 1-15 and 60-67, column 5, lines 65-67, column 6, lines 1-15, column 7, lines 29-37 and 65-67, column 8, lines 1-5 and 14-17, column 11, lines 11-45, "restriction types can include, for example, the number of times SPT 116 can be played back, a number of storage media such as storage medium 202 (Fig. 2) on which SPT 116 can be fixed, and the number of devices to which SPT 116 can be bound" and column 12, lines 60-67);

a digital content playing device used for at least playing the content file on the distributing recording medium and having a function of communicating via the communication line with the management unit, the piece data being necessary for the digital content playing device to play the data body, wherein when a request to play the content file under authentication and charging conditions is inputted by a user to the digital content playing device, the digital content playing device transfers the request via the communication line to the management unit, the management unit checks authentication and charging of the user related to the request before transferring the piece data via the communication line to the digital content playing device, and the digital content playing device uses the header information on the distributing recording medium and the piece data only in play operation to play the data body on the distributing recording medium (column 2, lines 6-45, "SPT is bound to a particular piece of storage medium by including data uniquely identifying the storage medium in a tamper-resistant form, e.g., cryptographically signed" and "Prior to playback of the SPT, the external player confirms that the media identification data has not been tampered with and properly identifies the storage medium" and lines 54-67, "authenticates the initiator using the certificate and responds with a reply message" and "initiator authenticates the responder using the certificate and responds with an exchange message", column 3, lines 1-15 and 60-67, column 4, lines 19-34, column 5, lines 40-67, column 6, lines 1-15 and 29-65, column 7, lines 65-67, column 8, lines 1-17 and 32-43, column 9, lines 58-67, column 10, lines 1-6 and 9-28 and column 12, lines 20-28 and 56-66).

7. Regarding claim 2, Ansell discloses a system for preventing unauthorized play of digital content comprising:

a distributing recording medium on which a content file having header information and a data body is recorded in a state of lacking at least part of the header information (column 5, lines 40-46, column 7, lines 65-67, column 8, lines 1-17, "parses header 302", column 11, lines 11-45, "specifying a type of restriction on playback of SPT 116", column 12, lines 56-67, "SPT 116 cannot be played back from any other storage medium unless cryptographic logic 1104 is accurately replicated" and column 13, lines 6-15);

a management unit for managing use of the content file on the distributing recording medium and capable of transmitting the prepared part of the header information as a piece data via a communication line (column 2, lines 6-13, 28-34 and 52-67, column 3, lines 1-15 and 60-67, column 5, lines 65-67, column 6, lines 1-15, column 7, lines 29-37 and 65-67, column 8, lines 1-5 and 14-17, column 11, lines 11-45, "restriction types can include, for example, the number of times SPT 116 can be played back, a number of storage media such as storage medium 202 (Fig. 2) on which SPT 116 can be fixed, and the number of devices to which SPT 116 can be bound" and column 12, lines 60-67);

a digital content playing device used for at least playing the content file on the distributing recording medium and having a function of communicating via the communication line with the management unit, the piece data being necessary for the digital content playing device to play the data body, wherein when a request to play the

content file is inputted by a user to the digital content playing device, the digital content playing device transmits the request via the communication line to the management unit, the management unit checks authentication of the user related to the request before transmitting the piece data via the communication line to the digital content playing device, and the digital content playing device uses the header information on the distributing recording medium and the piece data in play operation to play the data body on the distributing recording medium (column 2, lines 6-45, "SPT is bound to a particular piece of storage medium by including data uniquely identifying the storage medium in a tamper-resistant form, e.g., cryptographically signed" and "Prior to playback of the SPT, the external player confirms that the media identification data has not been tampered with and properly identifies the storage medium" and lines 54-67, "authenticates the initiator using the certificate and responds with a reply message" and "initiator authenticates the responder using the certificate and responds with an exchange message", column 3, lines 1-15 and 60-67, column 4, lines 19-34, column 5, lines 40-67, column 6, lines 1-15 and 29-65, column 7, lines 65-67, column 8, lines 1-17 and 32-43, column 9, lines 58-67, column 10, lines 1-6 and 9-28 and column 12, lines 20-28 and 56-66).

8. Regarding claim 3, Ansell discloses a distributing recording medium fabrication device used for the system for preventing unauthorized play of digital content according to claim 1, which separates piece data from a content file having header information and a data body for recording and records the content file separated from the piece data on a recording medium received in the preparation device to create a distributing recording

medium (column 2, lines 52-67, column 5, lines 40-67, column 6, lines 1-19 and 29-53, column 8, lines 7-18, column 9, lines 58-67, column 10, lines 1-8, column 12, lines 20-28 and 56-67 and column 13, lines 6-15).

9. Regarding claim 4, Ansell discloses a digital content playing device used for the system for preventing unauthorized play of digital content according to claim 1, which has functions of:

when a request to play the content file is inputted by the user, transmitting the request via the communication line to the management unit (column 2, lines 46-51, column 4, lines 45-52, "Each of user input devices 130 generates signals in response to physical manipulation by the listener and transmits those signals through interconnect 106 to processor 102", column 7, lines 29-38, column 8, lines 31-44, column 9, lines 32-41 and 58-67 and column 10, lines 1-18);

thereafter, when the piece data is transmitted from the management unit via the communication line, using the header information on the distributing recording medium and the piece data in play operation to play the data body on the distributing recording medium (column 8, lines 31-44, column 13, lines 62-67 and column 14, lines 1-12).

10. Regarding claim 5, Ansell discloses a recording medium storing playing software used for the system for preventing unauthorized play of digital content according to claim 1, wherein the digital content playing device is a computer and the playing software is processed by the computer (column 5, lines 40-46, column 7, lines 65-67, column 8, lines 1-17, "parses header 302", column 11, lines 11-45, "specifying a type of restriction on playback of SPT 116", column 12, lines 56-67, "SPT 116 cannot be played

back from any other storage medium unless cryptographic logic 1104 is accurately replicated" and column 13, lines 6-15),

wherein the system is made such that when a request to play the content file is inputted by the user, the request is transmitted via the communication line to the management unit, and thereafter, when the piece data is transmitted from the management unitvia the communication line, the header information on the distributing recording medium and the piece data are used in play operation to play the data body on the distributing recording medium (column 2, lines 46-51, column 4, lines 45-52, "Each of user input devices 130 generates signals in response to physical manipulation by the listener and transmits those signals through interconnect 106 to processor 102", column 7, lines 29-38, column 8, lines 31-44, column 9, lines 32-41 and 58-67, column 10, lines 1-18, column 13, lines 62-67 and column 14, lines 1-12).

11. Regarding claim 6, Ansell discloses a system for preventing unauthorized play of digital content comprising:

a delivery management unit delivering a content file having header information and a data body via a communication line and managing use of the data body (column 2, lines 6-13, 28-34 and 52-67, column 3, lines 1-15 and 60-67, column 5, lines 65-67, column 6, lines 1-15, column 7, lines 29-37 and 65-67, column 8, lines 1-5 and 14-17, column 11, lines 11-45, "restriction types can include, for example, the number of times SPT 116 can be played back, a number of storage media such as storage medium 202 (Fig. 2) on which SPT 116 can be fixed, and the number of devices to which SPT 116 can be bound" and column 12, lines 60-67);

a digital content playing device capable of communicating via the communication line with the delivery management unit and used for at least playing the content file delivered from the delivery management unit, wherein when a request to download the content file is inputted by a user to the digital content playing device, the digital content playing device transfers the request via the communication line to the delivery management unit, the delivery management unit transfers the content file related to the request via the communication line to the digital content playing device with the content file lacking a part of the header information to prevent unauthorized play and unauthorized copy thereof, thereafter, when a request to play the content file under authentication and charging conditions is inputted by the user to the digital content playing device, the digital content playing device transfers the request via the communication line to the delivery management unit, the delivery management unit checks authentication and charging of the user related to the request to transfer the prepared part of the header information as piece data via the communication line to the digital content playing device, and the digital content playing device uses the header information of the transferred content file and the piece data only in play operation to play the data body of the content file (column 2, lines 6-45, "SPT is bound to a particular piece of storage medium by including data uniquely identifying the storage medium in a tamper-resistant form, e.g., cryptographically signed" and "Prior to playback of the SPT, the external player confirms that the media identification data has not been tampered with and properly identifies the storage medium" and lines 54-67, "authenticates the initiator using the certificate and responds with a reply message" and "initiator

authenticates the responder using the certificate and responds with an exchange message", column 3, lines 1-15 and 60-67, column 4, lines 19-34, column 5, lines 40-67, column 6, lines 1-15 and 29-65, column 7, lines 65-67, column 8, lines 1-17 and 32-43, column 9, lines 58-67, column 10, lines 1-6 and 9-28 and column 12, lines 20-28 and 56-66).

12. Regarding claim 7, Ansell discloses a system for preventing unauthorized play of digital content comprising:

a delivery management unit which is a server in which a content file having header information and a data body is prepared in a state of lacking part of the header information and the part of the header information is prepared as a piece data, and which delivers the content file via a communication line and manages use of the data body (column 11, lines 11-18, column 13, lines 62-67 and column 14, lines 1-12);

and a digital content playing device capable of communicating via the communication line with the delivery management unit and used for at least playing the content file delivered from the delivery management unit, the piece data being necessary for the digital content playing device to play the data body, wherein when a request to download the content file is inputted by a user to the digital content playing device, the digital content playing device transmits the request via the communication line to the delivery management unit, the delivery management unit transmits the content file related to the request via the communication line to the digital content playing device (column 2, lines 46-51, column 4, lines 45-52, "Each of user input devices 130 generates signals in response to physical manipulation by the listener and transmits

those signals through interconnect 106 to processor 102", column 7, lines 29-38, column 8, lines 31-44, column 9, lines 32-41 and 58-67, column 10, lines 1-18, column 13, lines 62-67 and column 14, lines 1-12),

thereafter, when a request to play the content file is inputted by the user to the digital content playing device, the digital content playing device transmits the request via the communication line to the delivery management unit, the delivery management unit checks authentication of the user related to the request to transmit the piece data of the content file related to the request via the communication line to the digital content playing device, and the digital content playing device uses the header information of the transmitted content file and the piece data in play operation to play the data body of the content file (column 2, lines 6-45, "SPT is bound to a particular piece of storage medium by including data uniquely identifying the storage medium in a tamper-resistant form, e.g., cryptographically signed" and "Prior to playback of the SPT, the external player confirms that the media identification data has not been tampered with and properly identifies the storage medium" and lines 54-67, "authenticates the initiator using the certificate and responds with a reply message" and "initiator authenticates the responder using the certificate and responds with an exchange message", column 3, lines 1-15 and 60-67, column 4, lines 19-34, column 5, lines 40-67, column 6, lines 1-15 and 29-65, column 7, lines 65-67, column 8, lines 1-17 and 32-43, column 9, lines 58-67, column 10, lines 1-6 and 9-28 and column 12, lines 20-28 and 56-66).

13. Regarding claim 8, Ansell discloses a digital content playing device used for the system for preventing unauthorized play of digital content according to claim 6, which has functions of:

when a request to download the content file is inputted by a user, transmitting the request via the communication line to the delivery management unit (column 2, lines 46-51, column 4, lines 45-52, "Each of user input devices 130 generates signals in response to physical manipulation by the listener and transmits those signals through interconnect 106 to processor 102", column 7, lines 29-38, column 8, lines 31-44, column 9, lines 32-41 and 58-67, column 10, lines 1-18, column 11, lines 46-67, column 13, lines 62-67 and column 14, lines 1-12);

after the content file is transmitted from the delivery management unit, when a request to play the content file is inputted by the user, transmitting the request via the communication line to the delivery management unit (column 2, lines 46-51, column 4, lines 45-52, "Each of user input devices 130 generates signals in response to physical manipulation by the listener and transmits those signals through interconnect 106 to processor 102", column 7, lines 29-38, column 8, lines 31-44, column 9, lines 32-41 and 58-67 and column 10, lines 1-18);

thereafter, when the piece data is transmitted from the delivery management unit via the communication line, using the header information of the transmitted content file and the piece data in play operation to play the data body of the content file (column 2, lines 6-45, "SPT is bound to a particular piece of storage medium by including data uniquely identifying the storage medium in a tamper-resistant form, e.g., cryptographically

signed" and "Prior to playback of the SPT, the external player confirms that the media identification data has not been tampered with and properly identifies the storage medium" and lines 54-67, "authenticates the initiator using the certificate and responds with a reply message" and "initiator authenticates the responder using the certificate and responds with an exchange message", column 3, lines 1-15 and 60-67, column 4, lines 19-34, column 5, lines 40-67, column 6, lines 1-15 and 29-65, column 7, lines 65-67, column 8, lines 1-17 and 32-43, column 9, lines 58-67, column 10, lines 1-6 and 9-28 and column 12, lines 20-28 and 56-66).

14. Regarding claim 9, Ansell discloses a recording medium storing playing software used for the system for preventing unauthorized play of digital content according to claim 6, wherein the digital content playing device is a computer and the playing software is processed by the computer, and in which the system is made such that when a request to download the content file is inputted by the user, the request is transmitted via the communication line to the delivery management unit, after the content file is transmitted from the delivery management unit, when a request to play the content file is inputted by the user, the request is transmitted via the communication line to the delivery management unit (column 2, lines 46-51, column 4, lines 45-52, "Each of user input devices 130 generates signals in response to physical manipulation by the listener and transmits those signals through interconnect 106 to processor 102", column 7, lines 29-38, column 8, lines 31-44, column 9, lines 32-41 and 58-67, column 10, lines 1-18, column 11, lines 46-67, column 13, lines 62-67 and column 14, lines 1-12),

and thereafter, when the piece data is transmitted from the delivery management unit via the communication line, the header information of the transmitted content file and the piece data are used in play operation to play the data body of the content file (column 2, lines 6-45, "SPT is bound to a particular piece of storage medium by including data uniquely identifying the storage medium in a tamper-resistant form, e.g., cryptographically signed" and "Prior to playback of the SPT, the external player confirms that the media identification data has not been tampered with and properly identifies the storage medium" and lines 54-67, "authenticates the initiator using the certificate and responds with a reply message" and "initiator authenticates the responder using the certificate and responds with an exchange message", column 3, lines 1-15 and 60-67, column 4, lines 19-34, column 5, lines 40-67, column 6, lines 1-15 and 29-65, column 7, lines 65-67, column 8, lines 1-17 and 32-43, column 9, lines 58-67, column 10, lines 1-6 and 9-28 and column 12, lines 20-28 and 56-66).

15. Regarding claim 13, Ansell discloses the system for preventing unauthorized play of digital content according to claim 1, wherein the digital content playing device is a computer, provided that playing software processed by the computer is prepared in the management unit or the delivery management unit, when a request to download the playing software is inputted by the user to the digital content playing device, the digital content playing device transmits the request via the communication line to the management unit *or* the delivery management unit, the management unit or the delivery management unit transmits the playing software related to the request via the communication line to the digital content playing device, and the digital content playing

device downloads the playing software (column 4, lines 45-52, "Each of user input devices 130 generates signals in response to physical manipulation by the listener and transmits those signals through interconnect 106 to processor 102", column 5, lines 40-46, column 7, lines 29-38 and 65-67, column 8, lines 1-17 and 31-44, column 9, lines 32-41 and 58-67, column 10, lines 1-18, column 11, lines 11-45, "specifying a type of restriction on playback of SPT 116", column 12, lines 56-67, "SPT 116 cannot be played back from any other storage medium unless cryptographic logic 1104 is accurately replicated", column 13, lines 6-15 and 62-67 and column 14, lines 1-12).

16. Regarding claim 14, Ansell discloses a digital content unauthorized play prevention method, wherein provided that a content file having header information and a data body in a digital content playing device previously lacks a part of the header information, and that the part of the header information is prepared as piece data in management unit for managing use of the content file in the device and capable of communicating via a communication line with the device, when a request to play the content file under authentication and charging conditions is inputted by a user to the device, the device transfers the request via the communication line to the management unit, the management unit checks authentication and charging of the user related to the request to transfer the piece data via the communication line to the device, the piece data being necessary for the device to play the data body, and the device uses the header information of the content file and the piece data only in play operation to play the data body of the content file (column 5, lines 40-46, column 7, lines 65-67, column 8, lines 1-17, "parses header 302", column 11, lines 11-45, "specifying a type of

restriction on playback of SPT 116", column 12, lines 56-67, "SPT 116 cannot be played back from any other storage medium unless cryptographic logic 1104 is accurately replicated" and column 13, lines 6-15).

17. Regarding claim 15, Ansell discloses wherein the request to play the content file by the user is made under an authentication and/or charging condition of the user (column 2, lines 54-67, "authenticates the initiator using the certificate and responds with a reply message" and "initiator authenticates the responder using the certificate and responds with an exchange message", column 4, lines 45-52, "Each of user input devices 130 generates signals in response to physical manipulation by the listener and transmits those signals through interconnect 106 to processor 102", column 7, lines 29-38, column 8, lines 31-44, column 9, lines 32-41 and 58-67, column 10, lines 1-18, column 13, lines 62-67 and column 14, lines 1-12).

18. Regarding claim 19, Ansell discloses a digital content unauthorized play prevention method, wherein provided that a content file having header information and a data body in a digital content playing device previously lacks a part of the header information, and that the part of the header information is prepared as a piece data in management unit for managing use of the content file in the device and communicable via a communication line with the device, the piece data being necessary for the device to play the data body, when a request to play the content file is inputted by a user to the device, the device transmits the request via the communication line to the management unit, the management unit checks authentication of the user related to the request to transmit the piece data of the content file related to the request via the communication

line to the device, and the device uses the header information of the content file and the piece data in play operation to play the data body of the content file (column 2, lines 6-45, "SPT is bound to a particular piece of storage medium by including data uniquely identifying the storage medium in a tamper-resistant form, e.g., cryptographically signed" and "Prior to playback of the SPT, the external player confirms that the media identification data has not been tampered with and properly identifies the storage medium" and lines 54-67, "authenticates the initiator using the certificate and responds with a reply message" and "initiator authenticates the responder using the certificate and responds with an exchange message", column 3, lines 1-15 and 60-67, column 4, lines 19-34, column 5, lines 40-67, column 6, lines 1-15 and 29-65, column 7, lines 65-67, column 8, lines 1-17, "parses header 302", and 32-43, column 9, lines 58-67, column 10, lines 1-6 and 9-28 and column 12, lines 20-28 and 56-66).

19. (New) Regarding claim 20, Ansell discloses wherein the communication line connects via the Internet (column 4, lines 62-67 and column 14, lines 4-12).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

20. Claims 10-12 and 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ansell as applied to claim 1 above, and further in view of United States Patent Application Publication No. US 2004/0030912 to Merkle et al., hereinafter Merkle.

21. Regarding claims 10, 11 and 12, Ansell discloses wherein the digital content playing device has functions of: determining an elapsed period from the point of time at which piece data is transmitted from the management unit or the delivery management unit (column 3, lines 1-15, "an expiration time beyond which the SPT can no longer be played" and column 11, lines 19-33).

22. Ansell significantly discloses the claimed invention, as cited above. However, Ansell does not substantially disclose the claim limitations pertaining to "when the elapsed period reaches a predetermined period, deleting the transmitted piece data". Merkle discloses said limitations, as cited below.

23. Regarding claims 10-12, Merkle discloses when the elapsed period reaches a predetermined period, deleting the transmitted piece data (page 10, paragraph 89, "a message can be deleted at any time if the header criteria for the number of message passing handler entities or complete circuits or time are met").

24. The motivation to combine would be to "achieve various levels of protection against unauthorized modification and distribution of digital content" (*Merkle* – page 2, paragraph 12).

25. Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Merkle with the teachings of Ansell so that "a secure time stamp and comparison process is created and used to detect by analysis of time domain effects, evidence of system tampering, monitoring, modification and subversion" (*Merkle* – page 2, paragraph 17).

26. Regarding claims 16, 17 and 18, Ansell discloses wherein the digital content playing device has functions of: determining an elapsed period from the point of time at which, aside from piece data, the content file is transmitted from the delivery management unit (column 3, lines 1-15, "an expiration time beyond which the SPT can no longer be played" and column 11, lines 19-33).

27. Ansell significantly discloses the claimed invention, as cited above. However, Ansell does not substantially disclose the claim limitations pertaining to "when the elapsed period reaches a predetermined period, deleting the transmitted content file". Merkle discloses said limitations, as cited below.

28. Regarding claims 16-18, Merkle discloses when the elapsed period reaches a predetermined period, deleting the transmitted content file (page 10, paragraph 89, "a message can be deleted at any time if the header criteria for the number of message passing handler entities or complete circuits or time are met").

29. The motivation to combine would be to "achieve various levels of protection against unauthorized modification and distribution of digital content" (*Merkle* – page 2, paragraph 12).

30. Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Merkle with the teachings of Ansell so that "a secure time stamp and comparison process is created and used to detect by analysis of time domain effects, evidence of system tampering, monitoring, modification and subversion" (*Merkle* – page 2, paragraph 17).

Conclusion

31. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

32. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

33. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

34. The following United States Patents are cited to further show the state of the art with respect to secure content protection, such as:

United States Patent No. 6,507,908 to Caronni, which is cited to show secure communication with mobile hosts.

United States Patent No. 7,243,366 to Medvinsky et al., which is cited to show a key management protocol and authentication system for secure internet protocol rights management.

United States Patent No. 7,017,188 to Schmeidler et al., which is cited to show a method and apparatus for secure content delivery over broadband access networks.

United States Patent No. 7,162,642 to Schumann et al., which is cited to show a digital content distribution system and method.

United States Patent No. 7,222,104 to Tadayon et al., which is cited to show a method and apparatus for transferring usage rights and digital work having transferable usage rights.

35. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEREMIAH AVERY whose telephone number is (571)272-8627. The examiner can normally be reached on Monday thru Friday 8:30am-5pm.

36. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

37. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Jeremiah Avery/
Examiner, Art Unit 2431
/Syed Zia/
Primary Examiner, Art Unit 2431